

BETMAX ENTERTAIN N.V

V 1.0

**Manual and Regulations for combating
Money Laundering, the Financing of
Terrorism and Proliferation of weapon
and mass destruction**

Content

INTRODUCTION	2
KEY RESPONSIBILITIES	4
PROVISION OF EDUCATION AND TRAINING	5
TARGETED FINANCIAL SANCTIONS	5
DEALING WITH SANCTIONED PERSONS	6
PROCEDURES	6
RISK ASSESSMENT	7
A POLITICALLY EXPOSED PERSON	7
LOCATION OF PARTNER	8
AMOUNT OF FUNDS BEING TRANSACTED	8
NATURE AND FREQUENCY OF TRANSACTIONS	8
SOURCE OF FUNDS BEING TRANSACTED	9
PLAYER RISK MATRIX	9
POLICY AND PROCEDURES	11
IDENTIFICATION	11
ANONYMOUS ACCOUNTS	11
EVIDENCE OF IDENTITY FOR PARTICIPANTS	11
ENHANCED DUE DILIGENCE	13
SOURCE OF FUNDS AND WEALTH	13
KYC MATRIX	14
ONGOING MONITORING	14
ONGOING MONITORING OF TRANSACTIONS	14
ONGOING MONITORING OF IDENTITY	15
RECORD KEEPING AND RETRIEVAL OF RECORDS	15
RECORD OF TRANSACTIONS	15
RETENTION OF RECORDS	16
REPORTING OF AN UNUSUAL/SUSPICIOUS TRANSACTION	17
ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	18
MONEY LAUNDERING REPORTING OFFICER AND MONEY LAUNDERING COMPLIANCE OFFICER	18
STAFF EDUCATION, TRAINING, AND DEVELOPMENT	18
IMPORTANCE FOR AML/CFT/CFP RISKS	18
THE IMPORTANCE OF STAFF IN ML PREVENTION	18
STAFF KNOWLEDGE, TRAINING AND AWARENESS	18
INTEGRITY	19
TECHNOLOGICAL DEVELOPMENTS	19
PROCEEDINGS	19
OFFENCES	19
APPENDIX A SUSPICIOUS ACTIVITY REPORT	20

Introduction

The aim of this manual is to set out the policies, procedures, systems and controls necessary to meet the obligations of the Company that operates from Curacao and is held to compliance with National Ordinance on identification when rendering services (NOIS) and National Ordinance on the reporting of unusual transactions (NORUT).

With the publication of the National Decree supervisor identification when rendering services gaming sector and the National Decree supervisor unusual transactions gaming, the Curaçao Gaming Control Board (GCB) is tasked with the AML/CFT/CFP supervision of the gaming sector operating in and from Curaçao.

The procedures that are appropriate for the purpose of forestalling and prevention of money laundering include:

- Identification
- Record keeping
- Staff education, training and development
- Internal procedures including the reporting of suspicious transactions, both internal and external

It is the Company's policy that NOIS and NORUT obligations to prevent money laundering are to be met in full and the company is committed to meeting and where possible exceeding such obligations.

The Company will not continue established relationships with participants whose conduct gives rise to suspicion of involvement with illegal activities. The company will seek to terminate any participant relationship where the participant's conduct gives reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion to the Curacao Financial Intelligence Unit (FIU) and thereafter shall be undertaken in conjunction with the relevant Government of Curacao authorities and in accordance with Curacao custom and practice to avoid any risk of the Company committing a tipping-off offence.

The Company's policies and procedures are based upon the regulations referred below and associated guidance issued by the Curaçao Gaming Control Board.

The laws and Regulations are form the main legal basis for the Curacao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of Article 2 of the sanctions National Ordinance, containing implementation of the United Nations' Security Council Resolutions concerning

Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);

- National Decree for general measures, of the 10th of July 2015, for the implementation article 2 of the Sanctions National Decree containing implementation of the of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of Article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30)
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34)
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)

What is Money Laundering?

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- Placement. During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- Layering. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- Integration. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

What is Financing of Terrorism?

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act. The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity.

There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods like those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

What is Financing of Proliferation of weapons?

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

Key responsibilities

The Company's management is responsible for:

- The day-to-day compliance with AML/CFT/CFP obligations within the areas of the Company for which they are responsible.
- Ensuring that the MLRO / Compliance Officer is provided with prompt advice of unusual/suspicious transactions and other matters of significance.
- Providing the MLRO and AML/CFT/CFP Compliance Officer with the appropriate resources to fulfil their functions effectively.
- Ensuring that the MLRO / Compliance Officer has complete autonomy in the suspicious activity report evaluation process and unfettered access to information necessary to carry out that process.
- The Directors and MLRO / Compliance Officer will ensure that he/she is provided with or has access to the necessary resources to keep up to date with new money laundering requirements and developments.

MLRO / Compliance Officer is responsible for:

- Developing necessary policies, procedures, training and education of staff.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations and experience/advice from enforcement agencies.
- Representing the Company to all external agencies and any other third- party making enquiries in relation to money laundering prevention or compliance.
- Ensuring that all parts of the Company are complying with the stated policy and therefore monitoring operations and development of the policy to this end.
- Undertaking the internal review of all suspicions and determining whether such suspicions have substance and require disclosure to the FIU.
- All contact between the Company and the Authorities in respect of routine reports to law enforcement in respect of any specific investigations.
- Establishing the suspicious reporting process and ensuring that this process is understood by all staff.
- Maintenance of the register of internal and external disclosures and register of money laundering and financing of terrorism enquiries.

AML/CFT/CFP Compliance Officer is responsible for:

- Establishing, recording, maintaining and operating appropriate procedures and controls for monitoring and testing compliance with the AML/CFT/CFP legislation.
- Adopt policies which manage the risks identified by the Company's business risk assessment, monitor the performance of these policies and address any deficiencies identified.
- Submission of a report, on at least an annual basis, to the Company's senior management that describes:
 - Any new developments within the industry in relation to AML/CFT/CFP including updates to any legislation or regulatory guidance.

- o Any updates to the Company's internal AML/CFT/CFP procedures and policies.
- o Any activities relating to compliance with the NOIS and NORUT.

All employees are responsible for:

- Remaining vigilant to the possibility of money laundering.
- Reporting to the MLRO / Compliance Officer all knowledge or suspicions of money laundering.
- Complying fully with all money laundering procedures in respect of client identification, client monitoring, record keeping, vigilance and reporting.

Provision of Education and Training

All members of management and staff will receive initial training and on-going training at least on an annual basis or as and when required.

Targeted Financial Sanctions

Sanctions are restrictions used by international communities as part of an attempt to stop financial crime and terrorism. They are designed as attempts to change the behavior of a targeted country, regime or individuals where diplomatic efforts have failed. Sanctions can take the form of economic, trade, financial services, or international movement (travel bans) prohibitions. Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities.

UN Sanctions

The United Nations Security Council publishes the names of individuals and organizations subject to UN financial sanctions in relation to involvement with ISIL (Da'esh), I-Qaeda, and the Taliban. All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities. The UN has in place other sanction lists pertaining to other jurisdictions, entities, and individuals, including wider terrorist activity under UNSR 1373.

The UN consolidated sanctions list is available at the following link:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

EU Sanctions

The European Union applies sanctions or restrictive measures in pursuit of the specific Common Foreign and Security Policy (CFSP) objectives set out in the Treaty of the European Union. Restrictive measures imposed may incorporate UN Security Council sanctions or EU autonomous sanctions. The latter cannot be imposed against individuals or entities where there is no foreign policy dimension.

Link to the EU sanctions regimes: <https://www.sanctionsmap.eu/#/main>

The above-mentioned website also includes information about the UN sanctions regimes.

OFAC Sanctions

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on the US foreign policy and national security goals against targeted foreign countries and regimes; terrorists; international narcotics traffickers; and those engaged in activities related to the proliferation of weapons of mass destruction; and other threats to national security, foreign policy or the economy of the US. It is important to note that while US sanctions do not directly apply to non-US companies outside the US, the use of the US dollar currency automatically engages OFAC regulations. US prosecutors take the view that if a financial transaction has cleared in the US (as do all US dollar payments, in New York), the US has jurisdiction over the offence. OFAC publishes a list of 'specially designated nationals' or SDNs (known as the SDN List) whose assets are blocked and firms, including US persons, are generally prohibited from doing business with them.

The OF AC Sanctions List Search is available at the following link:

<https://sanctionsscarch.ofac.trcas.gov/>

Dealing with sanctioned persons

In case when the Employee during Client on-boarding, COD or EDD procedure, or during Client ongoing monitoring becomes in the possession of the information that the Client is a sanctioned individual or has any links to sanctioned individuals and/or entities, he MUST:

- Immediately freeze all the funds / economic resources of the Client available to the Company;
- Not enter into any financial transactions or provide financial assistance or services to the Client;
- Apply Enhanced Due Diligence measures;
- Immediately inform and file the internal report to the MLRO / Compliance Officer;
- Suspend the account of the Client until further instructions from the MLRO / Compliance Officer.

It is prohibited to inform the Client or any third party (except a senior manager or MLRO / Compliance Officer) in advance, that a freezing measure is to be applied.

The MLRO / Compliance Officer has to review the internal report as soon as practicable and, in case there are reasonable grounds to suspect that the Client is the sanctioned individual from the lists provided by OFAC, EU, UN or national Sanctions regimes, the MLRO / Compliance Officer will cease to conduct any further business and a report will be submitted to the FIU.

Procedures

- All persons conducting business with the Company are properly identified, that their identity is verified where appropriate and sufficient information is gathered and recorded to permit the Company to 'know its client' and predict the expected pattern of business.
- Potential new business partners that do not appear to be legitimate are declined and where there is suspicion relating to criminal conduct on the part of a declined participant such suspicion is reported to the Money Laundering Reporting Officer (MLRO / Compliance Officer).
- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations.
- Full co-operation is provided to the law enforcement authorities to the extent required by statute/regulation.

- All suspicions are reported promptly to the MLRO / Compliance Officer.
- That the Company's vigilance systems are implemented and regularly monitored.

Risk Assessment

Based on the FATF Recommendations, casinos are required to apply a Risk-based Approach when designing policies, procedures and controls to combat money laundering, financing of terrorism and financing of proliferation of weapons. As part of the company's regulated approach to AML/CFT/CFP risk the following assessment has been conducted to adopt a risk-based approach to compliance with customer due diligence, both at the point of registration and in relation to on-going monitoring of clients.

A Politically Exposed Person

A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting due to being considered more vulnerable to bribery and corruption.

Therefore, full enhanced due diligence must be conducted upon any identified PEPs. The Company does not distinguish between foreign and domestic PEPs, all are considered high risk. A PEP that no longer holds their prominent public role will also be deemed high risk.

Screening is undertaken by the Company to identify PEP and Sanctioned individuals upon customer registration/deposit. This will also pick up on any adverse media relating to the customer.

A PEP is defined as a natural person who is or has been entrusted with prominent public functions, including:

- A head of state, head of government, minister or deputy or assistant minister;
- A senior government official;
- A Member of Parliament (MP);
- A senior politician;
- An important political party official;
- A senior judicial official;
- A member of a court of auditors or the board of a central bank;
- An ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
- A high-ranking officer in an armed force;
- A senior member of an administrative, management or supervisory body of a State-owned enterprise;
- A senior official of an international entity or organization.

A PEP also includes family members and close associates of the above, including:

- A spouse;
- A partner considered by national law as equivalent to a spouse;
- Other known close personal relationships such as a partner, boyfriend or girlfriend;
- A child;
- A spouse or partner of a child;
- A brother or sister (including a half-brother or half-sister);
- A spouse or partner of a brother or sister;
- A parent;
- A parent-in-law;
- A grandparent;

- A grandchild;
- A joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with a PEP;
- The sole beneficial owner of a legal person or legal arrangement known to have been set up for the benefit of a PEP;
- A beneficiary of a legal arrangement of which a PEP is a beneficial owner or beneficiary;
- A person in a position to conduct substantial financial transactions on behalf of a PEP.

BetMax Entertain N.V. has made the decision to not accept PEPs as customers, as they fall outside the Company's risk appetite.

Location of Partner

A customer located in a jurisdiction which is not Financial Action Task Force ("FATF") compliant (named on FATF's List Black or Grey), may generally be considered to represent a potential risk of money laundering or terrorist financing activity.

Therefore, customers located in jurisdictions named within the Blacklist will be automatically subjected to enhanced due diligence and subject to a higher degree of monitoring.

Amount of funds being transacted

Casinos have the obligation to undertake Customer due diligence measures when:

- Players engage in cumulative financial transactions equal to or above EUR 2000,--
- Carrying out occasional transactions above the monetary equivalent of EUR 2000,--
- There is a suspicion of money laundering or terrorist financing; or
- They have doubts the veracity or adequacy of previously obtained customer identification data

If funds deposited or withdrawn by a customer are over EUR 2,000 (or currency equivalent) or aggregate in excess of EUR 2,000 (or currency equivalent) in any thirty day period (qualifying payment), there is an enhanced risk of money laundering or terrorist financing activities and identity verification checks are undertaken. Such customers will be deemed as a medium risk.

When a customer reaches the threshold, the transaction that they are attempting (either a deposit or withdrawal) will not be permitted until they have satisfied their standard or enhanced due diligence requirements accordingly.

Nature and frequency of transactions

Where an individual is making regular deposits and betting transactions there is considered only minimal potential risk of money laundering or terrorist financing, unless they reach the thresholds. Irregular patterns of activity or regular deposits and withdrawals with limited betting transactions may highlight enhanced risk both from an AML/CFT/CFP and social responsibility perspective. Participants managing their payments and withdrawals to remain non-qualifying may also represent enhanced potential risk.

The procedures detailed in the following pages address both the requirement to identify participants and to gather evidence verifying their identity but also to monitor on-going activity to determine a change in the risk profile of the participant.

Several changes to a customer's transactions may prompt an investigation, requiring the customer's identity to be verified and potentially for the customer's source of wealth to be established. Source of wealth checks will establish both the legitimacy of the customer's funds and as to whether they can afford their current levels of spending. Such checks will be conducted on a case-by-case basis.

Multiple accounts are not permitted on the platform. This risk is mitigated by the system automatically preventing registration with matching emails, usernames, first names and surnames. However, there is always the possibility that an individual has used false registration details or details that are not theirs to create several accounts. Multiple accounts can be used to carry out multiple smaller transactions to avoid triggering any due diligence thresholds. Ongoing monitoring practices will be utilized to analyze transactional patterns, similar registration details, matching IP and device data to detect multiple account abuse. In such circumstances these individuals will be automatically banned from the platform unless a reasonable excuse can be provided from the customer.

Source of funds being transacted

The source of the funds will be verified to be coming from a legitimate source with legitimate connections to the customer. Any contradictions to this will result in the customer's account being suspended either indefinitely or until a reasonable explanation is provided.

All withdrawals should be sent to the source from which the customer deposited. However, should the customer have a legitimate reason as to why this is not possible (e.g. the closure of a bank account), relevant documentation must be submitted by the player demonstrating the reason why the payment source is now not available, and that the customer is the owner of the new payment method.

Multiple changes to the source of funds when multiple transactions are being made should also be queried by the Company as this is a potential indicator of money laundering. Should the customer make a change of their source of funds 3 times, then they will be deemed medium risk and subjected to due diligence checks. Should the customer make a change of their source of funds 5 or more times, then they will be deemed high risk and subjected to enhanced due diligence checks.

Player Risk Matrix

Risk rating	Nature	Location	Source of funds/ Wealth	Transaction size
Prohibited	Sanctioned individual or entity A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply	Closed jurisdictions A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the	A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements	A customer that has breached any of the below thresholds but does not comply with the Company's CDD/EDD requirements

	with the Company's CDD/EDD requirements Anyone deemed to be linked with the financing of terrorism Business participant	Company's CDD/EDD requirements	Funds appear to be generated or linked to the proceeds of crime	
High	PEP Any individual or entities subject to warnings Professional gambler Customers that are sporting professionals betting on sports High net worth individuals	Named on FATF's Blacklist. Countries with AML/CFT/CFP strategic difficulties	Use of over 5 different deposit methods	Deposit or withdrawal of EUR 10,000 in any period (or currency equivalent)
Medium	Public profile raises some form of concern e.g. adverse media, social media activity	Named on FATF's List B. Countries which in the opinion of the MLRO / Compliance Officer represents heightened risk	Use of voucher or pre-paid card Where the method of withdrawal differs to that of original deposit Use of over 3 different payment methods	Deposit or withdrawal of over EUR 3,000 (or currency equivalent) or aggregate more than EUR 3,000 (or currency equivalent) in any 30-day period
Low	Individual	Fully compliant with FATF No AML/CFT/CFP concerns	Bank transfer Debit or credit card Approved payment service provider	Under any of the qualifying payment thresholds

Following the risk assessment, customers will be identified as either low, medium, high or will not be able to open an account. The relevant level of customer due diligence will then be applied to each participant's account and reviewed on an on-going basis as part of the monitoring procedure.

The Company will undertake a review of the relevance of its risk assessment as part of the AML/CFT/CFP Compliance Officer's annual report to senior management or as and when significant changes in business operations dictate.

Policy and Procedures

Identification

For casinos, verification of identity must be conducted when engaging in cumulative financial transactions equal to or in excess of EUR 2000.—(equivalent to XCG 4000,—). This implies that all CDD measures must have been conducted at the time the threshold is reached. The casino reserves the right to request photo ID, address confirmation or perform additional verification procedures (request selfie, arrange a verification call etc.) for the purpose of identity verification prior to granting any withdrawals. All withdrawals must be made to the original debit, credit card, bank account, method of payment used to make the payment.

However, casinos are required to apply a minimum level of CDD measures prior to reaching the threshold. Thus, simultaneously with the opening of an account, casinos are to identify the customer by collecting the minimum personal details.

Participants registering on the site are required to input a password of their choosing. No player under the age of 18 can register with the company. If their age is below 18, they are unable to register.

Records will be maintained by the Company's administration of all current, attempted and past registrations.

No monies can be deposited with the company and no bonuses allocated to the account until the account has been activated.

Anonymous Accounts

Customers will not be able to register with fictitious names or anonymous accounts.

When registering with a website owned by the Company, the account will not be opened unless the requested identity details (shown above) are completed in full. Duplicate accounts will not be allowed, and checks will be made at the time of registration.

Fictitious names will not be allowed. Obvious fictitious names will be identified at the time funds are deposited to the account and the account will be terminated.

A participant whose account is terminated will be advised by email unless it is in relation to a matter reported to the FIU, in which circumstances please be advised accordingly by the MLRO / Compliance Officer.

Evidence of identity for participants

Payments made to participants that cumulatively exceed EUR 2000 (or currency equivalent) trigger the requirement for evidence to be gathered confirming the registered participant's identity.

CDD measures to be taken are as follows:

- a) Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information
- b) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
- c) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, its source of funds

Verification of identity

The verification of identity may be completed via the verification screening conducted upon registration/first deposit depending on the information gathered. Should the screening report support enough information whereby the customer's name, address and date of birth can be relied on as being accurate then that will be sufficient for this purpose and no further information will be required from the customer. However, consideration must also be applied should there be any other suspicion, for example if you suspect that the customer is underage and is using the details of an adult to register on the platform. In such circumstances further due diligence items should be requested from the customer.

As part of the screening report, PEP, sanction and adverse media checks will also be made.

When requesting due diligence from a player, at a minimum the following information must be collected:

- Full name
- Identification document
- Permanent residential address
- Date of birth
- Place of birth
- Identity number

To be acceptable identity documents must be:

- A good clear high-quality color scanned copy, plainly legible,
- Unexpired at the date of receipt,
- Bear a photo of the holder, and
- Signed by the holder

Verification of address

- A recent account statement (i.e. no more than 6 months old) from a recognized bank, building society or credit card company or the most recent mortgage statement from a recognized lender.
- An unexpired photographic driving license or national identity card containing current residential address if the document has not been used to verify identity.

- A recent rate, council tax or utility bill (recent in respect of utility bills is for the last quarter i.e. no more than 6 months old). Mobile telephone bills are not acceptable as evidence of address under any circumstances.
- Correspondence from an official independent source such as a central or local government department or agency Known lawyer's confirmation of property purchase or legal document recognizing the title to the property.
- Documents provided to verify an address should not refer to P.O. Boxes or care of addresses.
- they appear to be under the age of 18 or of a different age that to that provided upon registration
- they appear to be linked to criminal activity or terrorist organizations

Enhanced Due Diligence

In certain cases, highlighted by the risk assessment, the Company may consider that a participant poses a higher risk. In these circumstances, enhanced due diligence will be requested and collected by the Company. Participants who pose an additional risk will be recorded as high risk within the administrative system and a report of their transactions and any other relevant information made available to the MLRO / Compliance Officer.

Enhanced due diligence will consist of the requirements as established for standard customer due diligence, in addition to the following:

- Requirement of additional identification data (middle names, former names, aliases, occupation, employer, personal identification number, previous addresses)
- Consideration as to whether this data needs to be further verified (additional identity documents, 'selfie' with the identity document, certified documents)
- Establish the source of funds
- Establish the source of wealth
- Flag the participant for enhanced on-going monitoring
- Open-source checks

A customer that is deemed high risk and has complied with all EDD requirements will be referred to a senior manager or the MLRO / Compliance Officer for approval before the customer is permitted to continue with any further activity on the platform.

A participant who poses a higher risk may be:

- a PEP
- Resident in a country which the company has reason to believe does not apply or insufficiently applies the FATF recommendations.
- Meets the EDD requirement on the risk matrix due to their level of transactions
- Meets the EDD requirement on the risk matrix due to the number of changes to their payment method.
- Any persons who are the subject of any warnings or notices.

Source of Funds and Wealth

Source of funds is quite simply the method by which the customer has deposited funds onto the platform. This should be easily identified upon the customer depositing, as the system should detect the method being used.

Should the system not recognize the payment method, is a method unauthorized to be used on the platform, or the payment details do not match with that of the registration, all activity on the account will be suspended and the matter reported to the MLRO / Compliance Officer.

Source of wealth is how a person has generated the money they are spending on the platform and their financial standing in general. When conducting enhanced due diligence, reasonable measures must be made to establish the source of wealth.

Documents may be requested from the customer to demonstrate their source of wealth, for example a pay slip or a contract of employment. Open-source checks can often shed light upon an individual's current employer. Each customer's source of wealth may differ entirely and therefore different approaches may need to be undertaken depending on the circumstances.

When reviewing the source of wealth information, the Company staff will need to consider how reliable or independent the source of the information is, how plausible the information is, and how this compares to the customer's activity.

KYC Matrix

The following matrix details the customer due diligence requirements:

Due Diligence Check	Low	Medium	High
PEP, Sanction and adverse media Screening	x	x	x
Identity Verification Screening	x	x	x
Request ID and address documents		x	x
Open source checks		x	x
Source of funds	x	x	x
Source of Wealth			x
Additional identity and address documents			x

Ongoing Monitoring

The casino must conduct ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they

are consistent with the casino, knowledge of the customer, the customer's business and risk profile.

Ongoing Monitoring of Transactions

All transactions by all customers are recorded and can be reported on a daily, weekly, monthly, or annual basis.

It is recognized that a significant change to the normal operation of an account could be a sign of suspicious activity. A change may be:

- Unusually large deposits based on past deposit history
- Unusual patterns in betting activity
- Large deposits followed by large withdrawals combined with minimal betting transactions
- Multiple changes to deposit and withdrawal methods

If during daily monitoring it is noted that a player's profile has altered in a way that would alter their risk level an immediate review would be undertaken to ensure that all due diligence criteria for the new risk level is met. Should any further documents or information be required the participant will be contacted with a request to provide such within a timely manner.

Transaction reports will be reviewed within fourteen (14) days and overseen by the MLRO / Compliance Officer and Senior Management. Where the activity is deemed to be unusual, an investigation into the customer may begin which may include asking the customer for their rationale for carrying out the activity or further information or evidence of the source of funds or source of wealth.

Ongoing Monitoring of Identity

Changes made to a customer's identity and personal information will be reported on to the Company management. The evidence of identity previously provided by the participant will be reviewed and steps taken to renew and update that information considering the reported changes to the participants identity.

In such circumstances, the verification procedures shall be followed in addition as to the customer providing reasoning for the change in details.

Should a customer's risk level increase (e.g. from low risk to medium risk) and due diligence documents are already held on the customer, consideration must be made whether further documents must be submitted. The previously supplied documents must be reviewed to ensure that they are not expired, in such circumstances up to date documents must be requested.

CDD/EDD held will be reviewed on an annual basis regardless of any changes to the customer's circumstances.

In the event that satisfactory confirmation of the information as to the identity of the participant or satisfactory verification of evidence of identity is not provided, then the account will be suspended, no further betting activity allowed, and consideration be given to the lodging of a suspicious transaction report.

Record keeping and retrieval of records

Record of Transactions

The Company will maintain appropriate records of all participants and their associated transactions. The MLRO / Compliance Officer has unfettered access to all records (other than those which are stored in an encrypted or hashed form) and reporting through the back-office computer system. All records and audit trails can be accessed by them and reported in hard copy format without delay and within 7 days of any request being made.

All internal compliance documents will be held on the back-office system, with the MLRO / Compliance Officer having full access.

Retention of Records

All the above-named records will be maintained in a secure and accessible form. Secure backups are made daily of the following customer data:

- Records
 - all registration details
 - identification verification details
 - standard and enhanced due diligence items
 - suspended accounts and reason for suspension
 - closed accounts
 - financial transactions – deposits, bets made, withdrawals, prize payments
 - self-exclusion periods (temporary and permanent)
 - self-imposed limits
 - excluded players
 - complaints and responses
 - audit trails
 - bank reconciliations
 - Customer Service electronic correspondence records

Records associated with a customer (including all identification records and the financial transactions made by them) are maintained for a period of 5 years after the date of closure of the customer's account or the date of the last transaction.

Records associated with the register of internal and external disclosures and the register of money laundering and financing of terrorism enquiries will be maintained for a period of 5 years following the finalization of the relationship with the related parties or for the period as advised by the FIU.

Reporting of an unusual/suspicious Transaction

An unusual transaction is a transaction inconsistent with the player's profile. Therefore the 1st key to recognize that a transaction or series of transactions is unusual is to know enough about the player. Suspicions must be reported to the MLRO / Compliance Officer as soon as reasonably practical. To make a report form as outlined in Appendix A can be used.

Receipt of the report will be acknowledged by the MLRO / Compliance Officer. It is necessary for the person making the report to include their name. Once an initial report has been submitted the person should continue to submit reports where further suspicious activity takes place, or if there are developments in respect of the matter originally reported.

The following transactions or intended transactions are deemed unusual:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice.
- Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55)
- Transactions in the amount of XCG 5,000 (equivalent EUR 3000, --) or more, regardless of form of payment.

Note; A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of XCG. 5,000 or more and is considered per gaming day. Also credit card transactions and e-wallet transactions are to be reported to the FIU.

The MLRO / Compliance Officer has full access to information and records of the company that the Directors consider necessary to evaluate internal reports received. They will document the evaluation process and the reasons for conclusions reached.

If after completing the evaluation process the MLRO / Compliance Officer considers that there is knowledge of, suspicion or reasonable grounds to suspect money laundering or terrorist financing the MLRO / Compliance Officer is responsible for:

- Submitting the necessary information to the FIU.
- Recording the disclosure in the register of disclosures.
- Dealing with subsequent production or account monitoring orders if there are any.

Tipping Off/Confidentiality

Any person must treat any information where that person knows or suspects that an unusual transaction report has been made or that an investigation is under way or proposed or strictly confidential.

No staff member may disclose to any person s/he has formed a suspicion that a person may be involved in suspicion that a person may be involved in suspicious matters or transactions or that a report has been lodged about that person with the FIU or any other authority.

Clear lines of reporting where matters or transactions are referred to the MLRO / Compliance Officer need to be maintained. All matters or transactions are to remain confidential between the reporting staff member and the MLRO / Compliance Officer.

It is an offense to disclose that an unusual transaction report or related information on a specific transaction has been reported to the FIU or that an investigation into money laundering, terrorist financing or the proceeds of crime is impending/pending, and to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

Anti-Money Laundering Compliance Program

An anti-money laundering program is an essential component of a casino's compliance regime. The primary goal of every good program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

The basic elements a casino must address is an anti-money laundering compliance program are:

- A system of internal policies, procedures and controls
- A designated compliance officer with day-to-day oversight over the AML program
- An employee screening program and ongoing employee training program, and
- An independent audit function to test the AML program

Money Laundering Reporting Officer and Money Laundering Compliance Officer

The Company shall always have an appointed MLRO / Compliance Officer and MLCO. The appointment of both roles will be sufficiently senior within the company and will have the right of direct access to the Directors of the Company and is independent from the games operations.

The MLRO / Compliance Officer and MLCO will have unfettered access to all reports, transaction histories, complaints and audit trails.

Staff education, training, and development

Importance for AML/CFT/CFP risks

The way the company is organized can increase or mitigate the exposure of the company to money laundering and terrorist financing risks. Procedures and controls operated by the company, many of which are required by law, can be applied to manage AML/CFT/CFP risk.

The Importance of Staff in ML prevention

Success in preventing money laundering and terrorist financing cannot be achieved by having appropriate policies alone. Even the best policies are useless if staff ignore or circumvent them, whether through ignorance, carelessness or deliberately. Staff are a business's strongest defense or their weakest link.

Staff Knowledge, Training and Awareness

Recruiting staff of integrity is not sufficient in of itself. Staff must have sufficient awareness and training to detect money laundering and terrorist financing and to understand what is expected of them.

It is key to effective AML/CFT/CFP arrangements that:

- Staff have sufficient knowledge or awareness to detect money laundering.

- Staff have sufficient training to know how to deal with cases once they know of or suspect money laundering.
- Staff are aware of their personal legal obligations.

Refreshment trainings will be arranged and to demonstrate compliance with the staff training requirements records will be maintained that include:

- Details of the content of the training programs
- The names of the staff members who have received the training
- The date on which the training was provided
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan

Integrity

The integrity of the directors and employees of the Company are the foundation of its AML/CFT/CFP measures. If staff lack integrity there is a danger that they may become involved in or become willing accomplices to laundering activity.

Direct involvement in laundering operations is the possible extreme. More likely is that staff without the right attitude are unlikely to:

- Maintain awareness and detect money laundering.
- Report money laundering if they become aware of it.
- Take seriously their own training or that of their subordinates.
- Encourage reporting and foster a culture that supports money laundering prevention.

Technological Developments

The Company recognizes the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism. As a consequence:

- The Directors retain a close eye on technological developments that are taking place particularly in relation to phishing activity, identity fraud, money laundering etc.
- In addition, the company has engaged with technology partners who are at the forefront of software and IT security and are engaged to maintain the on-going integrity of the website, servers and backup.
- The Company is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solutions.

Proceedings

Offences

Any person who contravenes the NOIS / NORUT rules in regard to the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT/CFP) will be reported to The Financial Intelligence Unit of Curaçao.

In determining whether a person has complied with any of the requirements of any part of NOIS / NORUT a court may take account of any relevant supervisory or regulatory guidance which applies to that person and which is given by the Gaming Control Board.

Contact

Should you wish to contact our Customer Service Department please send a request on support@bombastic.com.

Appendix A | Suspicious Activity Report

Report prepared by:	
Business partners	
Name	
Account ID	
Address	
Email address	
Telephone number	
Is identification and address verification held?	
Is enhanced due diligence held?	
Reason for suspicion	
To include: Identification verification Criminal conduct known or suspected	
Date of report	
Receipt of report acknowledged	
Signed MLRO / Compliance Officer	
Date	

Approval / Rejections				
Director	Signed		Date	
MLRO / Compliance Officer	Signed		Date	
Development Review				
Responsible Person Review of Development	Date			
	<i>Review to comment on whether the development has been implemented in accordance with the outlined previously on this Form and whether a further risk assessment should be conducted</i>			
Approved	Director 1 Signed		Date	
	Director 2 Signed		Date	